



Right to Digital Legacy: Ownership, Privacy, and Ethical Management of Digital Assets After Death

Dr. Santosh Kumar

B.Sc. (Maths), LL.M., NET, JRF, SRF, Ph.D. (LAW)

ARTICLE DETAILS	ABSTRACT
Research Paper	
Keywords : <i>Digital Legacy, Digital Assets, Posthumous Privacy, Data Ownership, Cyber Law, Human Rights, India, Artificial Intelligence</i>	<i>In the digital age, a person's existence extends far beyond the physical world. From emails, social media profiles, and online banking to digital art, photographs, and cryptocurrencies—our identities now inhabit virtual spaces. Yet, the law remains largely silent on what happens to these digital possessions when a person dies. The concept of the Right to Digital Legacy emerges as a critical human right, demanding recognition of an individual's ownership, privacy, and control over their digital assets, even posthumously. This paper examines the legal, ethical, and human rights dimensions of digital legacy management across global jurisdictions, with a focus on the Indian legal context. It explores the tension between privacy, consent, inheritance, and corporate control, urging the creation of a unified global framework to protect the dignity and autonomy of digital identities after death.</i>

Introduction

Human identity has undergone a paradigm shift in the 21st century. Life today unfolds simultaneously in physical and digital spaces. From personal communications and photographs to professional data and social media interactions, much of an individual's personality and memory now exists online. Death, however, does not erase these traces; the deceased continue to "live" digitally—through data, profiles, and digital assets that persist indefinitely.

The question then arises: who owns, manages, or controls a person's digital legacy after death? Can heirs inherit Facebook pages, Gmail accounts, or cryptocurrency wallets? Should personal messages remain private even posthumously, or can family members access them?



The Right to Digital Legacy deals precisely with such dilemmas. It embodies the individual's autonomy and dignity beyond physical death, encompassing ownership, privacy, and ethical management of digital remains.

This emerging right sits at the intersection of technology, human rights, property law, and ethics. It is a pressing issue for lawmakers, especially as digital dependence deepens and artificial intelligence begins to memorialize human existence through data.

This paper analyzes the conceptual foundations of the Right to Digital Legacy, its global legal developments, ethical and privacy implications, and the evolving Indian perspective. It argues that posthumous digital rights must be recognized as part of the continuum of human dignity and privacy.

Concept of Digital Legacy

The term digital legacy refers to the digital content, assets, and online records left behind by an individual after death. These may include:

- **Personal assets:** emails, photos, videos, documents stored on cloud services.
- **Social media accounts:** Facebook, Instagram, X (Twitter), LinkedIn, etc.
- **Financial assets:** online bank accounts, cryptocurrency wallets, PayPal, NFTs.
- **Intellectual property:** blogs, digital writings, art, research, and code.
- **Digital identities:** usernames, passwords, avatars, and AI-generated content.

A digital legacy is both personal and economic, combining sentimental value (memories, communication) and monetary worth (digital property).

While traditional property law governs tangible and intangible assets, digital assets pose novel challenges. They are stored on servers controlled by private corporations, governed by terms of service, and often inaccessible without passwords or legal authority.

Hence, managing digital remains involves not only inheritance but also posthumous privacy, consent, and ethical data governance.

Philosophical and Human Rights Foundations

The Right to Digital Legacy stems from fundamental human rights principles, notably:

1. **Human Dignity:** Every individual deserves respect even after death. The protection of digital remains continues the recognition of dignity beyond physical existence.



2. **Autonomy and Consent:** Individuals must decide what happens to their digital data after death—whether it should be preserved, deleted, or transferred.
3. **Right to Privacy:** Privacy does not automatically expire at death; certain aspects of informational privacy persist to protect the deceased's memory and family.
4. **Property and Ownership:** Digital assets constitute intellectual or virtual property and must be inheritable or transferable under the owner's will.
5. **Right to Be Forgotten:** Closely related, this right allows individuals to erase personal data online, extending conceptually to posthumous contexts.

These principles show that the Right to Digital Legacy is not a luxury but an essential part of the emerging human rights discourse in the information society.

The Nature of Digital Assets

Digital assets are unique because they are non-physical, globally stored, and contractually governed. Unlike land or gold, digital property often resides on servers owned by multinational corporations—Google, Meta, Amazon, or Apple—subject to private terms of service.

This creates a complex web of ownership: while users generate content, platforms control access. Legally, users have license rights, not absolute ownership. Hence, upon death, the right to access or transfer such content depends on contractual clauses and privacy policies, not inheritance laws.

For instance, Google's Inactive Account Manager allows users to decide what happens to their data after inactivity, while Facebook offers a "Memorialization" option. Yet these policies are corporate measures, not legal entitlements.

Thus, the recognition of digital legacy as a legal right is essential to shift control from private companies to individuals and their heirs.

Legal and Ethical Dimensions of the Right to Digital Legacy

1. Ownership and Inheritance

Traditional succession laws were crafted for tangible assets. The challenge today is whether digital content constitutes property capable of inheritance. Jurisdictions vary:

- The United States treats digital assets as inheritable under certain state laws like the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), 2015.



- In the European Union, inheritance of digital assets is guided by data protection and privacy principles under the General Data Protection Regulation (GDPR).
- India, however, lacks any statutory recognition of digital assets in inheritance law. The Indian Succession Act, 1925 does not define or govern digital property.

Ethically, ownership also raises moral questions: should heirs have unrestricted access to private conversations or personal data of the deceased? Balancing emotional closure and privacy becomes critical.

2. Posthumous Privacy

Privacy is traditionally seen as a right of the living, but in the digital age, it extends beyond death. Posthumous privacy protects the deceased's digital information from unauthorized access, alteration, or public disclosure.

Philosophically, this rests on the continuity of human dignity. Just as physical remains are protected from desecration, so should digital remains be safeguarded from exploitation.

Cases like the Facebook v. German Parents dispute (2012) highlight the tension. Parents sought access to their deceased daughter's Facebook messages, but the company refused citing privacy laws. Courts eventually ruled in favor of the parents, setting a precedent for balancing family rights and posthumous privacy.

3. Ethical Management of Digital Assets

Ethical management involves respecting the deceased's will, consent, and dignity. Tech companies must act as custodians—not owners—of user data. Ethical considerations include:

- Non-disclosure of sensitive data that could harm the deceased's reputation.
- Secure deletion of data as per user's instructions.
- Providing heirs limited access for memorial or legal purposes.
- Preventing misuse, defamation, or identity theft using deceased persons' data.

Digital ethics demands that human memory and identity not become commodities in the hands of corporations.

International Legal Framework

Although there is no dedicated international treaty on posthumous digital rights, several global instruments provide a foundation.



1. Universal Declaration of Human Rights (UDHR, 1948)

Article 12 ensures protection against arbitrary interference with privacy. Modern interpretation extends this principle to digital and posthumous contexts as part of the dignity continuum.

2. International Covenant on Civil and Political Rights (ICCPR, 1966)

Article 17 protects individuals from unlawful interference with privacy and correspondence. The UN Human Rights Committee has recognized that data privacy forms part of this protection.

3. General Data Protection Regulation (GDPR, EU, 2018)

While GDPR primarily protects living individuals, several EU nations like France and Italy have expanded its scope to include posthumous data management. Article 23 allows member states to legislate on the rights of deceased persons regarding personal data.

4. Council of Europe's Convention 108+ (2018)

This convention on data protection encourages member states to consider protection of personal data beyond life, ensuring that dignity continues after death.

5. UNESCO's Universal Declaration on the Human Genome and Human Rights (1997)

Although focused on genetic data, it establishes an ethical precedent that human data embodies dignity and must be treated with respect, even posthumously—a principle analogously applicable to digital data.

Judicial Precedents and Global Practices

Courts around the world have begun addressing issues concerning digital inheritance and posthumous data control.

- **Germany (2018):** In *Facebook v. Federal Court of Justice*, the court ruled that parents could inherit their deceased child's Facebook account, equating digital communications to letters and diaries.
- **United States:** Cases like *In re Estate of Ellsworth* (2005) recognized that digital accounts and emails are property subject to estate administration.
- **France:** Under its Data Protection Law (2016), individuals can specify directives for the management of their data after death.
- **United Kingdom:** The Law Society of England and Wales encourages inclusion of digital assets in wills, though no statutory framework yet exists.



- **Japan:** With rising concerns over digital inheritance, financial regulators have recognized cryptocurrencies as property that can be passed to heirs.

These examples demonstrate the global momentum toward recognizing digital legacy management as part of posthumous rights.

The Indian Legal Context

India stands at an early stage in addressing posthumous digital rights. Neither the Information Technology Act, 2000, nor the Indian Succession Act, 1925, deals with digital inheritance or privacy after death.

However, India's judiciary and policy frameworks are slowly recognizing digital privacy as a fundamental right and extending its logic to emerging domains.

1. Constitutional Foundation

Following the landmark judgment in Justice K.S. Puttaswamy v. Union of India (2017), privacy has been enshrined as a fundamental right under Article 21. The reasoning implies that digital data, being part of personal identity, deserves protection beyond life as an extension of human dignity.

2. Information Technology (IT) Act, 2000

The IT Act governs cyber offences and data protection but lacks provisions concerning posthumous data control. Sections 43A and 72A deal with data privacy, but these rights expire with the person.

3. Personal Data Protection Bill (2023)

The Bill introduces principles of data processing and consent but remains silent on what happens after the data subject's death. Thus, posthumous digital rights remain a grey area in Indian law.

4. Cultural and Ethical Considerations

Indian tradition deeply values the remembrance and respect of the deceased. Extending this reverence into the digital realm aligns with the constitutional morality of dignity and the spiritual ethos of śraddhā (reverence for ancestors). The protection of digital remains could be viewed as a modern manifestation of this moral duty.

Ethical Dilemmas and Moral Dimensions

The right to digital legacy is not merely a question of ownership or succession—it represents a deeper moral and philosophical challenge. The digital self of a person continues to interact, influence, and even



evolve after death. This persistence of digital identity creates unique ethical dilemmas that law alone cannot resolve.

1. Autonomy vs. Family Interests

One of the most contentious questions concerns the access of family members to the deceased's data. While heirs may claim emotional or financial reasons for accessing a loved one's digital content, such access can conflict with the deceased's privacy or the privacy of third parties involved in communication. For instance, personal emails, private photos, or confidential business communications may contain information that the deceased would not have wanted disclosed. The ethical principle of respect for autonomy dictates that a person's digital wishes—whether to delete or preserve data—must prevail over others' curiosity or emotional need.

2. Commercial Interests vs. Human Dignity

Corporations such as Meta, Google, or Apple hold vast repositories of personal data. After death, this data can have commercial value for targeted marketing, AI training, or algorithmic analysis. Ethical management requires these companies to treat digital remains not as property but as sacred memory—preserving dignity over profit.

3. Posthumous Identity and Deepfakes

Advances in artificial intelligence now allow creation of digital replicas—AI “chatbots” that mimic deceased persons using their data. While some find comfort in these “griefbots,” they raise moral questions about identity, consent, and emotional manipulation. Is it ethical to resurrect someone digitally without their approval? Can an AI avatar truly represent the deceased's will?

These dilemmas underscore the need for explicit consent during one's lifetime to determine the boundaries of digital resurrection and memorialization.

4. The Right to be Forgotten after Death

In digital environments, nothing truly disappears. Search engines and social media archive human presence indefinitely. The Right to be Forgotten—recognized under the EU's GDPR—should extend to the deceased, allowing designated persons or authorities to erase data that violates dignity or privacy.

This is particularly vital in cases of individuals wrongfully accused, victims of crime, or those whose online content could cause harm to surviving relatives.



Artificial Intelligence, Digital Resurrection, and Memory Ethics

AI and machine learning have redefined how society remembers the dead. Social media platforms curate “memorial pages,” AI models generate posthumous voices, and virtual reality reconstructs interactions with lost loved ones.

1. AI Memorialization

Facebook’s “Memorialization Feature” allows users’ profiles to remain active as digital memorials managed by “legacy contacts.” Similar services like Replika or HereAfter AI create AI versions of people who can “speak” to their families after death.

While these innovations offer emotional solace, they blur ethical lines between memory and simulation. They may perpetuate digital existence against the deceased’s will or distort their authentic identity.

2. Data Ownership in AI Models

AI training often uses vast amounts of user-generated data. When a person dies, their photos, writings, and voices may still feed into algorithms. This raises ownership questions: does the data belong to the deceased’s estate, the AI company, or the public domain? Without legal clarity, posthumous consent risks being ignored.

3. Emotional and Psychological Impact

Digital immortality challenges the grieving process. Scholars of digital ethics argue that interacting with AI versions of the dead can hinder emotional closure and create psychological dependency. Therefore, AI memorialization must be guided by ethics of empathy, authenticity, and respect.

Corporate Policies on Digital Legacy Management

Several major technology companies have adopted internal mechanisms to manage users’ data after death. While progressive, these remain contractual privileges rather than legal rights.

1. Google – Inactive Account Manager

Google’s system allows users to specify trusted contacts who will receive access to selected data if the account becomes inactive. Users may also choose to have data deleted after a period of inactivity.



2. Meta (Facebook and Instagram) – Memorialization

Facebook allows users to appoint a “Legacy Contact” to manage a memorialized profile, which remains viewable but cannot be logged into. The feature aims to respect the deceased’s memory while preventing misuse.

3. Apple – Digital Legacy Programme

Apple introduced the Digital Legacy feature in iOS 15, allowing users to assign “Legacy Contacts” who can access data stored in iCloud upon the user’s death.

4. Twitter (now X) and LinkedIn

These platforms permit verified family members to request account deletion but offer no inheritance rights.

While these corporate practices mark an ethical step forward, they rely on company discretion and lack uniform global standards. A codified legal right would ensure accountability and prevent arbitrary decisions.

The Indian Perspective: Emerging Legal and Ethical Challenges

India, with its rapidly expanding digital population, faces growing complexities around digital inheritance and posthumous data protection.

1. Legal Vacuum

Neither the **Information Technology Act, 2000** nor the **Digital Personal Data Protection Act, 2023** explicitly addresses posthumous data. Once a user dies, their account is governed solely by the platform’s policy, often based outside India. This creates jurisdictional uncertainty.

For instance, if an Indian citizen’s Gmail or Facebook account is hosted on servers in the U.S., disputes over access and privacy become transnational.

2. Succession and Property Law Issues

The **Indian Succession Act, 1925** and **Hindu Succession Act, 1956** govern inheritance of physical and intellectual property but do not include digital assets. Even cryptocurrency inheritance remains legally unclear.

Courts have not yet ruled on whether social media or email accounts can be part of an estate. In absence of legislation, digital rights after death depend on contractual consent rather than statutory entitlement.



3. Privacy and Dignity Post-Death

The Puttaswamy judgment (2017) laid the foundation for digital privacy as part of Article 21. Extending this principle, digital dignity should logically continue beyond life, ensuring protection against misuse, defamation, or unauthorized publication of a deceased person's content.

4. Cultural Dimensions

Indian ethos reveres remembrance and spiritual continuity. Practices such as śrāddha (ancestral homage) signify that the dead remain part of collective memory. In a digital society, this translates into the moral responsibility to preserve, not exploit, the digital remains of the deceased.

Comparative Jurisdictions and Lessons for India

- **United States:** The RUFADAA (2015) allows fiduciaries to manage digital assets of the deceased, balancing privacy with estate administration.
- **European Union:** GDPR's framework and national laws in France and Italy recognize posthumous directives.
- **Japan:** Recognizes digital currency as inheritable property, and tech companies have begun voluntary compliance.
- **Singapore:** The Personal Data Protection Commission has issued guidelines encouraging users to prepare "digital wills."

India could draw from these examples to create a hybrid model blending privacy protection, inheritance law, and technological accountability.

Challenges in Implementing the Right to Digital Legacy

1. **Absence of Legal Definitions:** There is no statutory definition of "digital asset" or "digital legacy," leading to interpretative ambiguity.
2. **Cross-Border Data Jurisdiction:** Digital assets are stored on foreign servers, complicating enforcement of national laws.
3. **Corporate Resistance:** Tech companies often resist sharing data, citing global privacy policies or user confidentiality.
4. **Lack of Awareness:** Most users are unaware of their ability to plan digital succession or define posthumous preferences.



5. **Cybersecurity Risks:** Data theft, impersonation, or unauthorized resurrection of profiles pose new threats to identity.

These challenges demand comprehensive legislation coupled with public digital literacy.

Recommendations for Global and Indian Policy Reform

1. Recognize Posthumous Digital Rights as Human Rights

Just as human dignity survives death in physical contexts, so must it persist digitally. International law should recognize posthumous privacy and digital inheritance under the broader umbrella of human rights.

2. Enact a Unified Digital Legacy Law

India should draft a Digital Legacy and Data Inheritance Act covering:

- Legal definition of digital assets.
- Procedures for nomination and consent during life.
- Recognition of digital wills and fiduciary access rights.
- Posthumous privacy safeguards and data deletion options.

3. Incorporate Posthumous Provisions in Data Protection Laws

Amendments to the Digital Personal Data Protection Act, 2023 could extend limited protection to the deceased's data, ensuring its ethical use.

4. Encourage “Digital Wills”

Citizens should be encouraged to create digital wills specifying how their data, online accounts, and digital currencies should be managed or deleted.

5. Establish Ethical Oversight

A National Digital Ethics Commission could oversee corporate compliance, prevent misuse of deceased persons' data, and formulate uniform guidelines.

6. Foster International Cooperation

Since data transcends borders, countries must collaborate to develop a Global Convention on Digital Legacy Rights under the UN or UNESCO framework.



Philosophical Reflection: Dignity Beyond Death

The Right to Digital Legacy is ultimately an affirmation that human dignity transcends mortality. It is the recognition that one's digital footprint—shaped by memory, creativity, and relationships—forms part of human identity deserving respect after death.

In moral philosophy, dignity is not contingent upon existence but on the inherent worth of the person. Just as societies protect graves and memorials, so must they safeguard digital memorials from distortion or misuse.

This perspective aligns with both secular human rights and Indian cultural ethics, where remembrance (smṛti) and respect (mān) constitute moral duties.

Conclusion

In the contemporary digital civilization, the boundary between life and afterlife has blurred. Individuals now leave behind not just wills and estates, but emails, social profiles, and entire digital ecosystems. Yet, the law remains anchored in an analog age.

The Right to Digital Legacy thus emerges as a new frontier of human rights, combining privacy, property, and dignity. It calls for balancing autonomy with inheritance, and technology with morality. From a global standpoint, the principle is clear: digital death should not mean digital erasure, but neither should it imply uncontrolled immortality. Ownership, access, and deletion must be guided by the expressed will of the deceased.

For India, integrating digital legacy within constitutional values of dignity and privacy under Article 21 would represent both legal progress and cultural continuity. Enacting dedicated legislation, recognizing digital wills, and aligning with global ethical standards would ensure that the digital self receives the same respect as the physical one. In essence, to protect digital legacy is to preserve humanity's memory with dignity, ensuring that technology serves remembrance—not exploitation. The future of digital civilization depends not only on innovation but also on how respectfully we manage the echoes of the past in the virtual realm.

References

1. Universal Declaration of Human Rights, 1948, Art. 12.
2. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
3. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.



4. Facebook v. Federal Court of Justice, Germany, Case No. III ZR 183/17 (2018).
5. Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), USA, 2015.
6. Digital Personal Data Protection Act, 2023 (India).
7. UNESCO, *Report on Ethical Issues of Posthumous Data*, 2021.
8. Luciano Floridi, *The Ethics of Information*, Oxford University Press, 2013.
9. European Court of Human Rights, *S. and Marper v. UK* (2008).
10. Law Society of England and Wales, *Guidance on Digital Assets in Estate Planning*, 2021.